Information Security Unit
Policy and Evaluation Division

Information Security Audit

TABLE OF CONTENTS

INTRODUCTION

This audit of information security operations at was conducted by the Information Security Unit (ISU), Policy and Evaluation Division (PED) between the period of .This auditor utilized the California Penal Code (PC), California Code of Regulations (CCR) Title 15 Division 3, the California Department of Corrections' (CDC) Department Operations Manual (DOM), and Administrative Bulletins (AB) as the primary sources of operational standards. In addition, applicable information security protocols were used in this audit as a benchmark for standardization.

This audit was conducted by the ISU.

The audit consisted of on-site inspection, interviews with staff, reviews of procedures and other documentation, and observation of institutional information security practices.

The purpose of this audit is one of overall analysis and evaluation of the institution's compliance with the terms and conditions of State regulations and information security standards.

AUDIT SCOPE AND METHODOLOGY

The purpose of this audit was to assess the level of compliance with established State regulations and departmentally-established standards in the areas of information security operations. This audit and the attached findings represent the formal audit of 's compliance by the PED.

The scope and methodology of this audit were based upon written audit procedures developed by the PED Information Security Unit and provided to staff in advance of the audit.

Random sampling techniques were employed as an intrinsic part of the audit process.

For the purpose of this audit, the auditor toured the institution. Randomly selected on-duty staff at all levels from medical, counseling, management, administrative, and custody areas were interviewed regarding current practices.

A random sample of 's Associate Information Systems Analyst's (AISA) files were reviewed, including inventory, disaster recovery plans, as well as maintenance and procurement records. Utilizing "point-in-time" methodology, files were evaluated against all administrative requirements pertaining to the documents contained in those files.

SUMMARY OF FINDINGS

Issues were found in the following areas:

A description of each of these findings is in the narrative portion of this report.

SCORING CATEGORIES

The chart beginning on the next page (page vi) shows the findings in each of the possible ratable areas, including those areas that are not ratable or not applicable.

Each of the items are rated as to whether or not the institution is in compliance. The chart utilizes the following symbols to denote compliance ratings:

RATING	DEFINITION
Compliance (C)	The requirement is being met.
Partial Compliance (PC)	The institution is clearly attempting to meet the requirement, but significant discrepancies exist.
Noncompliance (NC)	The institution is clearly not meeting the requirement.
Not Applicable (NA)	Responsibility for compliance in this area is not within the authority of this institution.
Not Rated (NR)	No measurable instances.

At the end of the chart is a Statistical Summary of Audit Findings. This summary presents a mathematical breakdown of compliance by total items and percentages (%).

CHART OF FINDINGS

AUDIT STANDARD	AUDIT FINDING 1999	AUDIT FINDING 2001	PAGE NO.
I. AUTOMATION SYSTEMS SUPPORT			
1. Institution Electronic Data Processing (EDP) Responsibility			
2. Institutional AISA Responsibility			
3. Inventory			
A. Records kept			
B. Accurate and up-to-date			
4. Modem Policy			
A. Modem utilized according to DOM?			
B. Accurate and up-to-date inventory?			
5. Software License Agreements			
6. IT Procurement & Justification			
7. Maintenance and Repair			
A. PC maintenance & repair records kept?			
B. Service performed in accordance with DOM?			
8. Virus Protection			
9. Disaster Recovery Plan (DRP)			
A. DRP in Place			
B. DRP Tested			
10. Application Development			
A. Applications not supported by Information Systems Division			
B. Who Developed the Program?			
C. If Inmate Developed, was he/she Supervised?			
11. Confidential Data			
A. Confidential/Sensitive information on other systems			
B. Who is Doing the Transfer?			
C. How is Data Being Transferred?			

	D. What System is it Transferred To? 12. Workgroup Computing (Internet & Networks) A. Request For Access B. Locations C. Inmate-Restricted Areas? D. Inmate access to these workstations? E. Passwords F. Password Maintenance			

	IV. COMPUTER REFURBISHMENT	1999	2001	Page
	IV. INMATE EDUCATION A. Inmate Supervision B. Diskettes/CDs Controlled by Instructor C. DOS Commands Removed D. Electronic Communications (Modem)			
V. I	**PIA COMPUTERS AND COMPUTER USE** **Supervision of Inmates' Use of Computers** **Section A – Physical Verifications and** 1. Staff responsible for supervision of inmates 2. Are inmate work areas clearly marked? 3. Staff PCs clearly marked "No inmate access"? 4. Inmate work areas fully visible to staff? 5. Outside communications in the area? (Phones, modems, fax machines) 6. Inmates using PCs on a network? (If yes, complete Section C) **Section B: Supervisors' Interviews** 7. Inmates screened for computer crimes and 8. Inmate diskettes clearly marked? 9. Inmate hard drives and floppy diskettes checked for data integrity and/or misuse on a regular basis? 10. Control system for floppy diskettes 11. Inmates have access to confidential, sensitive or personal information? **Section C: Network Administrator (applicable only if inmates use networked PCs)** 12. Are staff using the same network? 13. Inmate access limited to only programs they use to complete their assignments? 14. Inmates allowed to do administration functions? 15. Outside communications on the network? 16. User logons, software, etc. setup?			

	17. Inmates access shared folders or drives on the			
	18. How are passwords managed for inmates?			
II.	**Manufacturing and Planning System (MAPS)**			
	1. Inventory			
	A. Lists from Property Unit and ISD match?			
	B. Actual device locations match ISD listing?			
	C. Frame Relay Access Device located in a secure location?			
	2. MAPS User Accounts and Logons			
	A. User IDs current?			
	B. Signed Security form for every user?			
	C. Security forms current?			
	D. Inmate users screened for computer fraud and crime?			
	E. Unauthorized access attempts?			
	F. Staff aware of logon procedures			
	G. Inmates aware of logon procedures			
	H. System Administrator and Backup assigned?			
III.	**Information Security Coordinator (ISC)**			
	1. ISC assigned?			
	2. Job description match duties of an ISC?			
	3. Network administrator training?			
	4. Disaster Recover Planning			
	a. Plan in place			
	b. Last time the plan was tested			
	5. Software licenses maintained			
	6. Procurement			
	7. Storage system for software disks?			
	8. Computer use agreements and self-certification forms?			

	9. Inmate-developed programs, databases, screensavers, etc. In use?			
	10. How are modems maintained?			
	11. Internet access allowed from any PIA area?			
	12. Inventory maintained			
	a. Staff computer inventory			
	1. Inventory maintained?			
	2. Inventory accurate and current?			
	3. Unauthorized software found?			
	b. Inmate-assigned computers			
	1. File content relevant to PIA work assignments (Detective check)?			
	2. "Inmate Access Allowed" signage?			
	3. Location, tag number and assigned user(s) correct?			
	4. GASP inventory verification			
	5. CABS directories removed?			
	6. Communications software present?			
	7. Network protocols and dial-up networking programs present?			
	8. Proscribed DOS (ATTRIB, DEBUG, ASSIGN) commands found?			
	9. Games found?			
	10. Computer monitors visible to staff?			
	11. Diskettes or CDs found in inmate work area?			
	a. Media clearly labeled as inmate work			
	b. System or installation media?			
	c. Content of and diskettes or CDs found in inmate work area?			
	12. Books, tools or computer components in the area?			
	IV. Information Security Training and Self-Certification			
	13. Logon IDs and Passwords			
	A. Staff have their own Logon/ID and password?			
	B. Users aware of information security practices?			
	C. Users aware of how to change passwords?			
	14. Information Security Training			
	15. Information Security Incident Reporting			

	A. Users aware of what constitutes an incident? B. Users aware of procedures? 16. Unattended workstations/terminals in work area?			

COMPARATIVE STATISTICAL SUMMARY CHART

2001 AUDIT FINDINGS

Possible Ratable Areas	Areas Rated in Each Audit	Areas Not Rated	Score

Audit Areas	Ratable Areas	Ratable Compliance	Partial Compliance	Non Compliance	Not Applicable	Not Ratable	
2001 Audits							
Automated Systems Support	26						
DDPS Applications	10						
Institutional PC Applications	21						
Computer Refurbishment Program	23						
Inmate Education	4						
Prison Industries Authority	66						
Totals							
1999 Audits							
Automated Systems Support							
DDPS Applications							
Institutional PC Applications							
Computer Refurbishment Program							
Inmate Education							
Prison Industries Authority							
Totals							
1998 Audits							
Automated Systems Support							
DDPS Applications							
Institutional PC Applications							
Computer Refurbishment Program							
Inmate Education							
Prison Industries Authority							
Totals							

Audit of Information Security

SUMMARY OF FACILITIES AUDITED

For the purpose of the audit, the auditor toured the institution, inspected records, and interviewed staff to determine the degree of compliance with established departmental policies, procedures, guidelines, and relevant information security standards.

I. AUTOMATION SYSTEMS SUPPORT

1. Institution Electronic Data Processing (EDP) Responsibility

Each Warden and Regional Parole Administrator is ultimately responsible for the security and utilization of all automated systems and databases in the respective facility or region. This includes the integrity and accuracy of data entered and the physical security of the data, hardware, and the system itself.
(DOM Section 41020.4)

Who does the Associate Information Systems Analyst (AISA) report to?

Findings

2. Institutional AISA Responsibility

Under the direction of the Warden or designee, or Regional Administrator or designee, the facility or region AISA is responsible for the coordination of automated systems issues for the facility. This position acts as the primary contact for Headquarters on automation-related issues, including Personal Computers PCs, the DDPS, and all other automated system concerns. Technical assistance and direction is provided by the Institutions Division Automation Support Unit. Assistance with DDPS issues is also provided by IASU [Institutions Automation Support Unit] and PASU [Parole Automation Support Unit].

This position is responsible for coordination of staff training on PC applications and systems, justification and acquisition of PC equipment through use of the PC policy, local automated system application support, inmate access to computers, on-site user assistance, information system security, and QC [Quality Control]

oversight and review coordination for all databases located in the area of assignment.
(DOM Section 41020.4)

Does the scope of the AISA's duties reflect those described in the policy?

Findings

3. EDP Inventory

The EDP inventory shall include the following data elements:

- Primary Location: division/branch, facility, or parole region where equipment is located.
- Secondary Location: unit or office where equipment is located.
- Brand of Equipment: monitors, keyboards, printers, etc.
- Model Number: monitors, keyboards, printers, etc.
- Serial Number: monitors, keyboards, printers, software, etc.
- Ownership: whether CDC or specified other owns.
- Version Number: software.
- Date of Acquisition: date equipment was received.
- Date of Installation: date equipment/software was installed.
- Date of Relocation: date equipment/software was relocated.
- Relocation Location: unit or office where equipment has been relocated.
- Signature: signature of local AISA or designee or AISA's supervisor.

(DOM Section 46030.4)

A) Is an inventory kept by the AISA?

Findings

The CDC shall maintain an inventory of its significant microcomputer commodities used for workgroup computing configurations. The inventory shall provide a description of each item (including serial and model numbers of equipment and version numbers of software), its date of acquisition, and the unit to which it is currently assigned. This inventory may be part of CDC's existing inventory system. The CDC shall also maintain inventories of licensed software and significant applications installed on workgroup computing configurations. These inventories will be available for audit purposes.
(DOM Section 48010.14)

B) Is the inventory complete and up-to-date?

Findings

4. Modem Policy

The acquisition of modems for use within the CDC shall be in compliance with the Department's PC and modem policies and the applicable sections of the Public Contract Code and SAM.

In addition, the following restrictions apply to modem use within facilities, parole offices, or any area that may be accessed by an inmate or parolee:

- There shall be no inmate or parolee access to PCs which have been approved for use of a modem.
- There shall be no inmate-developed programs on PCs with modems.
- There shall be no inmate or parolee access to Local Area Networks containing modems.
- Modems shall not be purchased as part of a PC acquisition without complying with the Department's modem policy.
- Internal and pocket modems shall not be purchased or used within the facilities. In addition, internal and pocket modems shall not be purchased or used in regional parole offices or units unless the PC utilized is located and operated in a secure area which cannot be accessed by parolees. (NOTE: internal modems may be installed in laptop PCs assigned to headquarters and parole personnel as long as the equipment:
  1. remains under the physical protection of designated personnel,
  2. is locked in a secure area/vehicle when not in use, and
  3. cannot be accessed by unauthorized users.
- Pocket modems used currently in the facilities shall be recalled and external modems substituted in their place.

Each facility and parole office is to develop a policy to ensure the security of modems used within that facility or parole office. The policy shall include procedures to ensure that:

- All modems are safeguarded when in use and protected from unauthorized access when not in use. External modem procedures shall include a plan to physically lock external modems when not in use.
- The physical location of each modem is tracked at all times.
- An on-site evaluation of modem use is performed no later than 90 days after installation of each modem installed in a facility. This on-site evaluation shall be conducted by Institutions Division or P&CSD staff, respectively.
  (DOM Section 48010.5, 48010.6)

A) Are modems utilized in accordance with DOM?

Findings

B) Is the inventory of modems complete, accurate and current?

Findings

5. Software License Agreements

Software license agreements shall be strictly adhered to. Proprietary software cannot be duplicated, modified, or used on more than one machine, except as expressly provided for in the manufacturer's license agreement Program updates may be downloaded from the Internet in accordance with the owner's license agreement.

(DOM Section 48010.10.1)

Are software license agreements strictly followed?

Findings

6. Procurement and Justification

The purpose of this policy is to ensure that the Department is in compliance with all control agency requirements. The ultimate authority for approval of information technology projects lies with the Office of Information Technology (OIT), but it is the intention of the Director of OIT to delegate such approval authority selectively, to the maximum extent practicable, to the departmental director. Refer to State Administrative Manual (SAM) Section 4819.34 for the factors considered by OIT in determining whether a project can be delegated. IS proposals to be funded with existing monies (no new positions) shall receive departmental and, if necessary, control agency review and approval before project development can proceed

If the procurement request is not covered by the Workgroup Computing Policy, the requesting unit shall complete a Feasibility Study Report (FSR). The Project Initiation Unit located in the Information Systems Branch (ISB) will provide assistance in completing FSRs.

During the acquisition of workgroup computing technologies, a procurement process will follow and/or parallel the workgroup computing authorization process.

Responsibilities of Procurement:

- The necessary procurement documents are completed and the acquisition is completed in conformance with the Public Contract Code and departmental policies and procedures.
- Information technologies procurements have been authorized. For workgroup computing technologies, this means ensuring that the Workgroup Computing Coordinator has an approved CDC Form 1855 on file, and that the procurement documents have appropriately referenced this Form.

(DOM Sections 43020.2, 43020.3.2, 45040.3, 48010.4.8; 48010.8; 48010.8.3)

Are Information Technology acquisitions conducted appropriately?

Findings

7. Maintenance and Repair

EDP equipment maintenance shall be performed by State personnel, or performed by maintenance service organizations in the private sector whose services are acquired through competitive bidding or as a sole source.

The CDC shall make provisions for necessary routine maintenance, as well as for the repair of malfunctioning equipment. It is the responsibility of workgroup management to budget necessary funds for maintenance and to ensure that maintenance schedules are met.
(DOM Section 48010.13, 46020.1)

A) Are PC maintenance and repair records kept as required?

Findings

B) Are PC maintenance and repair services performed by State personnel or by private sector organizations?

Findings

8. Virus protection

The CDC staff must also be aware that computer viruses pose a potentially serious threat to departmental computer and information assets. Virus protection must be implemented on every departmental workstation. The ISD, Network Services Unit, is responsible for defining and/or maintaining the infrastructure for these security systems. The user is responsible for following the established processes that are defined.
(DOM Section 48010.9)

Is virus protection implemented in accordance with ISD's guidelines?

Findings

9. Disaster Recovery Plan (DRP)

It is the policy of the California Department of Corrections (CDC) that each element of the Department utilizing information technology shall establish disaster recovery planning processes for identifying, assessing, and responding to the risks associated with its information assets. See the Department Operations Manual (DOM), Section 49010 for additional details.
(DOM Section 49040)

The Department operational recovery plan shall cover a minimum of four topic areas:

- Summary of the strategy for managing disaster situations.

- Distinct management and staff assignment of responsibilities immediately following a disaster and continuing through the period of normal operations re-establishment.
- Priorities for the recovery of critical applications.
- Operational procedures documented in systematic fashion that shall allow recovery to be achieved in a timely and orderly way.

A) Is there a DRP in place for the institution?

Findings

B) When was the plan last tested?

Findings

10. Applications Development

The person responsible for supervising inmate programmers at each site shall certify in writing that the policies relating to inmate programmers are being adhered to at their specific site.

A copy of this certification shall be kept on site by the local security coordinator. **(DOM Section 49020.19.7)**

A) Are there any applications in this institution not supported by Information Systems Division (ISD)?

Findings

B) Who developed the program?

Findings

C) If an inmate developed the program, was he/she properly supervised during the development?

Findings

11. Confidential Data

Information maintained on workgroup computing configurations shall be subjected to the same degree of management control and verification of accuracy that is provided for information maintained in other automated and manual files within CDC, as defined in the appropriate sections of the DOM.

If a data file is downloaded to a workgroup computing configuration from another computer system, the requirements for information integrity and security that

have been established for the data file shall be adhered to while it is stored at the workgroup level.

Electronic transfer (file transfer) of information to or from any CDC information system file or database is restricted to authorized persons who shall use an approved file transfer mechanism. The confidentiality and integrity of the information shall be protected within the computer environment to which the information has been transferred.
(DOM Sections 48010.9.2, 49020.16)

A) Is there <u>confidential</u> or sensitive information on a system that has electronic file transferred data?

<u>Findings</u>

B) If A) is yes, who is doing the information transfer?

<u>Findings</u>

C) If A) is yes, how is the data being transferred?

<u>Findings</u>

D) If A) is yes, what other system is it being transferred to?

<u>Findings</u>

12. Workgroup Computing

Establish policy structures, levels of approval, and accountability to define the appropriate use, acquisition, and support (maintenance and training) of workgroup computing technologies, including electronic mail functionality and Internet access. The basis for the workgroup computing justification is the CDC Form 1855, which is maintained by the Workgroup Computing Coordinator and is modeled after the form shown in SAM Section 4991. The CDC Form 1855 is used to justify the acquisition of workgroup computing technologies. The form is also used to request and gain approval for Internet browsing access.
(DOM Section 48010.2, 48010.8.1, 48010.8.2)

Each procurement of a workgroup computing technology, is subject to management review and approval before an actual order can be placed or the unit takes possession of the equipment or software. Approval is required to gain Internet access or to establish an Internet or Intranet Web page. In addition to the standard lists maintained by the Workgroup Computing Coordinator, ISD maintains the standards for network infrastructures, including Local Area

Network's, Wide Area Network's, and Internet/Intranet connections. To ensure network interoperability and consistency within CDC, ISD's networking group will review and approve requests that involve new network installations, Internet access requests, Intranet Web pages, and exceptions to departmental standards. Units proposing to acquire workgroup computing commodities are expected to select from these lists whenever possible.
(DOM Section 48010.8, 48010.6)

The CDC Form 1857, must be on file for each employee using workgroup computing technologies, accessing departmental networks, and/or accessing the Internet. It is the policy of CDC that each new employee completes the CDC Form 1857 as part of their employee orientation process. The CDC Form 1857 should be maintained in the employee's official personnel file.
(DOM Section 48010.8.2)

Acquisition of additional workgroup computing capabilities for previously acquired configurations are subject to similar reviews and approvals. Requests for Internet access will be processed in the same manner as acquiring other workgroup computing technologies, with the same approvals. Internet and Intranet Web page requests will also follow the approval process as shown above.
(DOM Section 48010.8.3)

Additional approvals are needed for exceptions to standards, new network installations, Internet access, remote access to the departmental systems and network and/or modem usage. These additional levels of approval have been defined in the appropriate sections of this policy.
(DOM Section 48010.8.3)

Users granted access to the Internet shall be required to abide by the acceptable use standards and shall have sufficient training in accordance with this and other policies related to electronic communications.
(DOM Section 48010.12)

Access to CDC's dedicated computers is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. User IDs shall never be shared. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what the password is.
- Not write down the password.
- Not use an obvious password.
- Not leave an active terminal session.

(DOM Section 49020.9.2)

Inmates shall not access any computer connected to a local area network (LAN), except as approved by the ISO; nor shall inmates access any computer which has

any type of direct, outside communication capability, except as provided in section 3370c.
(California Code of Regulations, Title 15, Section 3041.3b)

Inmates shall not access any computer that contains or is capable of accessing, or is connected to, other computers containing sensitive or confidential informatin, except as provided in section 3370b.
(California Code of Regulations, Title 15, Section 3041.3e)

No communication capabilities; e.g., telephone lines, data lines, or telephone access punch panels, shall be permitted in any area where inmates are allowed to access computers, except as approved by the ISO.
(California Code of Regulations, Title 15, Section 3041.3k)

A) Are all requests for Workgroup Computing solutions and "Request For Access" to the Internet using the CDC form 1855?

Findings

B) Where are the workstations approved under Workgroup Computing located?

Findings

C) Are any of these workstations that are either connected to a network or have outside communications capability, including Internet access, located in areas where inmates have access?

Findings

D) Are inmates allowed to access networked or Internet-capable workstations?

Findings

E) Does each user have their own user ID/password?

Findings

F) How are User IDs and passwords maintained?

Findings

II. DEPARTMENTAL SYSTEMS (DISTRIBUTED DATA PROCESSING SYSTEMS – DDPS)

1. Distributed Data Processing Systems (DDPS) Responsible Staff

DDPS is a system comprised of one or more minicomputers operating in each facility and connected to minicomputers in headquarters via a wide area communications network. Four major applications reside currently on the DDPS. In addition to the requirements of this section, use of each application shall meet general operating specifications regarding policy, purpose, responsibility, QA [Quality Assurance], and QC.
(DOM Section 47130.4)

The following system applications may be randomly audited for compliance:

DDPS APPLICATION	RESPONSIBILITY
Inmate Roster Movement System	Control Sergeant
Inmate Classification System	Correctional Counselor II
Inmate Assignment System	Inmate Assignment Lieutenant
Inmate Trust Accounting System and Checkwriter	Trust Officer
Inmate Canteen System	Canteen Manager
Inmate Tuberculosis Alert System	Medical Staff
Automated Visiting Information System	Visiting Lieutenant
Inmate Mental Health Identifier System	Medical/Psych. Services

Who is the person responsible for data input for each application?

Findings

2. Inmate Access

Inmates shall not have access to any computer containing sensitive or confidential information. In addition, computers containing sensitive or confidential information shall have appropriate hardware or software security measures installed.
(DOM Section 42020.6)

A) Are inmates involved in the process, or do they have access to the work area?

Findings

B) Is there an appropriate "ACCESS" emblem posted on the terminal or workstation?

Findings

3. Logon/IDs and Passwords

Access to CDC's dedicated computers is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. Authorized persons engaging in a terminal session with a computer shall log off (terminate the session) before leaving the immediate vicinity of the terminal, because the password which allowed the session to begin remains in effect throughout the session. Additionally, no ability shall exist for a user to store, load, or invoke the logon process on any CDC computer, by any method that includes the user Resource Access Control Facility (RACF) ID or the password. Violation of this policy may result in the revocation of all access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those having used the password. User IDs shall never be shared. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what the password is.
- Not write down the password.
- Not use an obvious password.
- Not leave an active terminal session.

(DOM Section 49020.9.2)

A) Do staff have their own logon/ID and personal password?

Findings

B) Are users aware of the necessary measures taken to ensure security and protection of information?

Findings

C) Are users aware of how password changes are handled?

Findings

4. Information Security Awareness

All persons who have access to any CDC information shall be provided security awareness training at the time such access begins, and at least annually thereafter.

All individuals having access to CDC information shall be made aware of the background, scope and objectives of CDC's information security program and of specific CDC information security policies and procedures that are applicable to the level and type of access granted to the individual.

All CDC employees shall also be made aware of the events and activities that constitute threats to the organization for which they work, and of the actions to be taken when confronted by those events or activities.
(DOM Section 49020.17)

A) ***When was the last time the user received security awareness training?***

Findings

5. Incident Reporting

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. It is the policy of the Department that the following incidents shall be reported through the chain of command to the departmental ISO:

- Any incidents involving unauthorized access to automated data, automated files, or databases.
- Any incident involving the unauthorized modification, destruction or loss of automated data, automated files, or databases.
- Any incident involving a virus, worm, or other such computer contaminant (see also DOM Section 41010).
- Any incident involving the unauthorized use of computer equipment, automated data, automated files, or databases.
- Any incident involving the misuse of the information assets of the Department.

(DOM Section 49010.6.2)

A) ***Are users aware of the type of "actions" which constitute an information security violation or incident which must be reported through the chain of command to the CDC ISO?***

Findings

B) Are users aware of the procedure for handing a suspected incident?

Findings

7. Information Integrity

The vast majority of information maintained by CDC is confidential and/or sensitive in nature. Its untimely or unauthorized release external to the organization may have significant, adverse impact on CDC.

Authorized persons engaging in a terminal session with a computer shall log off (terminate the session) before leaving the immediate vicinity of the terminal. User IDs shall never be shared
(DOM Section 48010.9.1, 49020.9.2)

Are there any unattended terminals or workstations with action sessions in the work area visited by the auditor?

Findings

III. PERSONAL COMPUTER SYSTEMS

1. Personal Computer System Applications

It is the policy of the California Department of Corrections (CDC) to provide, where appropriate, Personal Computer (PC) applications as an alternative to other types of information technology or manual systems. Ease of maintenance, cost effectiveness, and efficiency are major considerations in determining the use of personal computers. Security is the primary policy consideration in initiating and maintaining all personal computer systems with sensitive information.
(DOM Section 47040.1)

The following PC applications may be randomly audited for compliance:

PC APPLICATION
PPAS - Post Assignment System
PPAS – Time Keeping
PPAS – Security Program
Fair Labor Standards Act Program (including 7k calculation module)
Automated Release Date Tracking System
Automated Transfer System
Inmate Appeals Tracking System
Critical Case Management System
State Logistics and Materials Management System
PC Food Manager Program
Pharmacy Prescriptions Tracking System
Reception Center Mental Health Screening (Reception Centers only)
Controlled Armory Tracking System
TB Chronolog Program
Watch Office Tracking System
In-Service Training
Tru-Time (PIA System)

A) Who is the person responsible for data input for each application?

Findings

B) What version of the software is installed on the workstation?

Findings

2. Inmate Access

Inmates shall not have access to any computer containing sensitive or confidential information. In addition, computers containing sensitive or confidential information shall have appropriate hardware or software security measures installed.
(DOM Section 42020.6)

A) Are inmates involved in the process?

Findings

B) Is there an appropriate "ACCESS" emblem posted on the workstation?

Findings

3. Training

Workgroup management is responsible for ensuring that staff members possess the knowledge and skills necessary for effective use of workgroup computing facilities, and that there is sufficient depth of training to prevent disruption of key activities in the event of unexpected staff changes. At least two staff members should be trained in using each workgroup computing application and the equipment that it uses.
(DOM Section 48010.12)

Are at least two staff trained in using the computer system and each application?

Findings

4. Equipment, Data and Application Integrity

In order to maintain the integrity of EDP information and ensure the security of equipment, the following policies shall be adhered to:

- All EDP hardware and software shall be for official use only.
- Reasonable measures shall be taken to locate equipment in a secure area, to provide protection from vandalism or sabotage, and to preclude access by other-than-authorized personnel.
- All microcomputers located in facilities and parole offices shall be equipped with a keylock mechanism that controls the power source to the processor and disk drives. If a keylock mechanism is not included with the microcomputer, then a keyboard or power lock shall be purchased separately and used. When not in use,

the key shall be removed from the lock.

- All microcomputers located in facilities and parole offices shall be associated with locking storage cabinets for software, manuals, and small peripheral equipment. Such equipment shall be secured in the cabinet(s) when not in use.
- A complete set of standard documentation shall be maintained by the individual or unit using the EDP equipment, and shall remain in an area immediately adjacent to the EDP equipment. Such documentation shall include:
  - All manuals supplying documentation relating to the installation, maintenance, or care of the equipment.
  - All manuals supplying documentation relating to the installation and use of proprietary software, except that such manuals may be located in a central library, if appropriate.
- There shall be no inmate access to EDP equipment connected in a Local Area Network (LAN) or having any type of direct, outside communication capability, unless approval is obtained from the Management Information Systems (MIS) Committee and CDC Information Security Officer.

(DOM Section 46010.4)

A) Where is the PC documentation pertaining to hardware, proprietary software, user-programmed applications, and all procedural documentation maintained?

Findings

B) Is there a mechanism to lock the power source and/or keyboard? Is the key removed from the lock when the computer is not in use?

Findings

C) Is the computer located in an area reasonably secure from theft and/or vandalism?

Findings

D) Is the computer used for authorized CDC business only?

Findings

5. Confidential Data

Electronic transfer (file transfer) of information to or from any CDC information system file or database is restricted to authorized persons who shall use an approved file transfer mechanism. The confidentiality and integrity of the information shall be protected within the computer environment to which the information has been transferred.

(DOM Section 49020.16)

A) Are data from this confidential system used elsewhere?

Findings

B) If A) is yes, who is doing the information transfer?

Findings

C) If A) is yes, how are the data being transferred?

Findings

D) If A) is yes, are the data provided the security and protection at least equal to the originating system?

Findings

6. Logon/IDs and Passwords

Access to CDC's dedicated computers is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. Authorized persons engaging in a terminal session with a computer shall log off (terminate the session) before leaving the immediate vicinity of the terminal, because the password which allowed the session to begin remains in effect throughout the session. Additionally, no ability shall exist for a user to store, load, or invoke the logon process on any CDC computer, by any method that includes the user Resource Access Control Facility (RACF) ID or the password. Violation of this policy may result in the revocation of all access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those having used the password. User IDs shall never be shared. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what the password is.
- Not write down the password.
- Not use an obvious password.
- Not leave an active terminal session.

(DOM Section 49020.9.2)

A) Do users have their own logon/ID and personal password?

Findings

B) Are users aware of the measures taken to ensure security of passwords?

Findings

C) Are users aware of how password changes are handled?

Findings

7. System Backup

Provisions shall be made to safeguard against the loss of information and programs stored on workgroup computing configuration as a result of product failures or power failures. Copies of all data files and software shall be stored in a safe location. A regular schedule for making backup copies of all data files shall be established. Unit Supervisors shall ensure that backup procedures are carried out.

Backup files of confidential data shall be maintained in a locked cabinet away from the location of the microcomputer containing the program providing access to such files.

(DOM Section 48010.9.3, 49020.16)

A) How often are files backed up?

Findings

B) Where are the backup disks stored?

Findings

8. Information Security Awareness Training

All persons who have access to any CDC information shall be provided security awareness training at the time such access begins, and at least annually thereafter.

All individuals having access to CDC information shall be made aware of the background, scope and objectives of CDC's information security program and of specific CDC information security policies and procedures that are applicable to the level and type of access granted to the individual.

All CDC employees shall also be made aware of the events and activities that constitute threats to the organization for which they work, and of the actions to be taken when confronted by those events or activities.
(DOM Section 49020.17)

A) When was the last time the user received security awareness training?

Findings

9. Incident Reporting

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. It is the policy of the Department that the following incidents shall be reported through the chain of command to the departmental ISO:

- Any incidents involving unauthorized access to automated data, automated files, or databases.
- Any incident involving the unauthorized modification, destruction or loss of automated data, automated files, or databases.
- Any incident involving a virus, worm, or other such computer contaminant (see also DOM Section 41010).
- Any incident involving the unauthorized use of computer equipment, automated data, automated files, or databases.
- Any incident involving the misuse of the information assets of the Department.

(DOM Section 49010.6.2)

A) Are users aware of what types of "actions" constitute an information security violation or incident which must be reported through the chain of command to the CDC ISO?

Findings

B) Are users aware of how a suspected incident is handled?

Findings

IV. COMPUTER REFURBISHMENT

The policy for the handling of donated computer equipment shall be standardized at every CRP site and shall be in compliance with the DOM, Sections 49020, 52040, 53090 and 53091, as stated in AB 94-16.

All CPUs shall be opened and searched for contraband and weapons before being brought into the secure perimeter. A location outside of the secure perimeter shall be provided for CRP to conduct a search of the donated equipment.

All communications peripherals (network cards, modems, etc.) shall be removed before the CPU is brought into the secure perimeter. Communications cards shall be stored outside of the secure perimeter in a located area after they have been removed. When requested, communications cards may be redistributed to schools with the completed refurbished systems, or they may be recycled. It shall be the responsibility of the school, not the refurbishing site, to install communications devices, drivers or any additional software. Schools must be notified that CRP does not warrant or provide network services or network drivers.

All hard drives shall be removed before the CPU is brought into the secure perimeter. A secure location shall be provided for the formatting of all donated hard drives. All donated hard drives shall be formatted by CRP free staff only. No inmates shall be allowed in the immediate area during the formatting process. No information shall be copied from donated hard drives to any other media, for any purpose. When possible, all hard drives shall be low-level formatted, or unconditionally high-level formatted before inmates are given access to the hard drive.

Only operating systems, applications software and diagnostic utility programs, approved in writing by headquarters CRP staff, are authorized for use at any refurbishing site. Individual licenses for diagnostic utility programs must be available in each refurbishing shop where it is being used. Use of approved diagnostic software in each CRP shall not exceed the licenses available at that site. Site licenses are acceptable; however, the original diskettes or CD-ROMs and the license specifying the quantity of licensure must be available in the shop location.

The operation of this program must meet the intent of the DOM, Subsection 49020.19, to ensure tightly controlled inmate access to computers. The intent of this program, to place donated, refurbished computers in schools (public, private, and government supported), requires close monitoring of the program and inmate access to the computers, computer diagnostic software, other computer software and all computer parts.
(AB 94/16, and ID Policy Memo 5/12/00)

A. Does the Institution have an OP that reflects the policies of the CRP?

Findings

B. Is there a location outside of the secure perimeter where all donated equipment is initially received?

Findings

C. Receiving and processing of all donated equipment prior to it entering the secure perimeter.

1. Does staff open and search all CPUs outside of the secure perimeter?

Findings

2. Does staff remove all communications devices (modems and network card) during the receiving process?

Findings

3. Does staff remove all hard drives from the CPUs during the receiving process?

Findings

D. Storage of components.

1. Is there a secure storage area located outside the secure perimeter for CPUs and components?

Findings

2. Are Communications devices (network cards and modems) stored in this location after they are removed during the receiving process?

Findings

E. ***Hard Drives.***

1. Are all hard drives formatted in an inmate-restricted area by CPR staff?

Findings

2. Is any information copied from donated hard drives prior to their being reformatted?

Findings

3. Are all donated hard drives low-level formatted or completely overwritten prior to inmates having access to them?

Findings

F. Software Licensing.

A) How are licenses for diagnostic and utility software maintained?

Findings

B) How are software media (disks and CD-ROMs) controlled?

Findings

G. Inventories, Tracking and Reports.

1. How are computers and components logged into the CRP?

Findings

2. How are inventories and tracking status maintained?

Findings

3. How are non-usable components reported as salvage?

Findings

***H.* Shop Procedures**

1. Are all inmate work areas clearly visible to CRP staff?

Findings

2. How are tools, including diagnostic software, controlled?

Findings

3. Are all non-necessary equipment and components removed from inmate work areas?

Findings

4. What software is copied onto the refurbished hard drives? How is this done?

Findings

5. How are communications devices handled during the refurbishment process?

Findings

6. Is there an unclothed body search of all inmates when exiting the CRP area?

Findings

I. What process is used for the disposal of salvage computers and parts?

Findings

J. Does the AISA receive the inventory of all diskettes and tools?

Findings

V. Inmate Education Computers

Inmate Access
Inmates shall not have access to any computer containing sensitive or confidential information. In addition, computers containing sensitive or confidential information shall have appropriate hardware or software security measures installed.
(DOM Section 42020.6)

Inmate Access To Computing
Computers are used in inmate academic/vocational education training programs. It is essential that the security of the facility be maintained and that no unauthorized communication is made by a computer to another computer or to an electronic mail device. In addition, data integrity and systems security shall be maintained at each work location. Each Warden, Regional Parole Administrator, and Deputy Director shall be responsible for computer resources and information security within their respective facility or division.

All facilities with inmates accessing computers in any capacity, including inmate education programs, shall comply with the following procedures:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Areas where inmates are authorized to work on computers shall be posted as such.
- There shall be no communication capabilities such as telephone, computer line, or radio communication devices in the area.
- Inmates shall not have access to utility programs such as Mace, Norton Utilities, or PC Tools.
- Inmates shall not have access to the MS-DOS commands DEBUG, ASSIGN, and ATTRIB.
- Inmates performing data entry or word processing in an authorized education or work production area should be supervised by staff persons able to identify and use the computer operating system, software, and application used on the equipment under their supervision.

  Inmates shall not remove diskettes from authorized work areas. An inventory and appropriate controls shall be maintained on all diskettes. Diskettes for inmate use shall be labeled "For Inmate Use." Reports and other printed output from inmate-utilized computers shall be reviewed closely by staff and appropriate distribution of such output shall be monitored.
  (DOM Section 42020.6)

A) Are inmates supervised according to DOM?

Findings

B) Does the instructor control diskettes and CDs?

Findings

C) Are the MS DOS® commands ATTRIB.EXE, DEBUG.EXE, ASSIGN.EXE removed from the PC hard drives of inmate accessible systems?

Findings

D) Are there electronic communications in the area?

Findings

VI. PRISON INDUSTRY AUTHORITY (PIA) COMPUTER USE

Audit of Information Security

Correctional Training Facility

GLOSSARY

AB	Administrative Bulletin
ABDDB	Abhorrent Bed Days Database
ABE	Adult Basic Education
ADMS	Automated Disciplinary Management System
Ad Seg	Administrative Segregation
AFMP	Automated Food Manager Program
AISA	Associate Information Systems Analyst
ARDTS	Automatic Release Data Tracking System
ASP	Avenal State Prison
ATA	Annual Training Agreement
ATS	Automated Transfer System
ARDTS	Automated Release Date Tracking System
AW	Associate Warden
ATS	Automated Transfer System
BIOS	Basic Input Output System
CAC	Commission on Accreditation for Corrections
CADDIS	Census and Discharge Data Information System
CAL	Calipatria State Prison
CASAS	Education Application
CATS	Controlled Armory Tracking System
CBM	Correctional Business Manager
CC	Correctional Counselor
CC	California Civil Code
CCC	California Correctional Center
CCI	California Correctional Institution
CCMS	Critical Case Management System
CCR	California Code of Regulations
CCR	Correctional Case Records
CCWF	Central California Women's Facility
CD	Compact Disk
CDC	California Department of Corrections
CDC 128-B	General Chrono Form
CDC 128-G	Classification Chrono Form
CDC 954	Interoffice Requisition-local
CDC 1166	Information Security Agreement
CDC 1167	Request to Access Information
CDC 1855	Workgroup Computing Justification
CDC 1857	Computing Technology Use Agreement
CDW	Chief Deputy Warden

CEN	Centinela State Prison
CIIMS	Correctional Institutional Information Management System
CIM	California Institution for Men
CISCO	**find**
CIW	California Institution for Women
CLETS	California Law Enforcement Telecommunications System
CMC	California Men's Colony
CMD	Contract Monitoring Database
CMF	California Medical Facility
CMO	Chief Medical Officer
CMOS	Computer Memory Operating System
CMOS	Complimentary Metal Oxide Semiconductor
CO	Correctional Officer
COR	California State Prison, Corcoran
C&PR	Classification and Parole Representative
CPU	Central Processing Unit
CRAFTS	Case Records Automated File Tracking System
CRC	California Rehabilitation Center
CRM	Community Resources Manager
CRP	Computer Refurbishment Program
CSP	California State Prison
CTF	Correctional Training Facility
CVSP	Chuckawalla Valley State Prison
DDPS	Distributed Data Processing System
DOM	Department Operation Manual
DOS	Disk Operating System
DRP	Disaster Recovery Plan
DVI	Digital Vision Inc.
DVI	Deuel Vocational Institute
EDP	Electronic Data Processing
EIPU	Education and Inmate Programs Unit
EMT	Employee Master Table
EOS	Emergency Operations Section
ERA	Employee Record of Attendance
ERO	Employee Relations Officer
ET	Electronics Technician
FLSA	Fair Labor Standards Act
FMLA	Family Medical Leave Act
FMS	Food Management System
FRAD	Frame Relay Access Device
FSP	Folsom State Prison
FSR	Feasibility Study Report
GASP	Automated Software Inventory Tool
GC	Government Code
GED	General Education Development
HazMat	Hazardous Materials
HCM	Health Care Management

HCSD	Health Care Services Division
HDSP	High Desert State Prison
HCCUP	Health Care Cost Utilization Review
IASU	Institutions Automation Support Unit
IATS	Inmate Appeals Tracking System
IB	Informational Bulletin
ICC	Institution Classification Committee
ICS	Inventory Control Sheet
ID	Identification
IE	Inmate Education
IGI	Institution Gang Investigator
I/M	Inmate
I/O	Input and Output
IPO	Institution Personnel Officer
IS	Information System
IS	Information Security
ISB	Information Systems Branch
ISC	Information Security Coordinators
ISD	Information Systems Division
ISO	Information Systems Office
ISO	Information Security Officer
ISP	Ironwood State Prison
IST	In-Service Training
ISU	Information Security Unit
ISU	Information Systems Unit
ISU	Investigations Security Unit
IT	Information Technology
LAC	California State Prison, Los Angeles County
LAN	Local Area Network
LT.	Lieutenant
MAPS	Manufacturing and Planning System
MCSP	Mule Creek State Prison
MDB	**find**
MIS	Management Information System
MHTS	Mental Health Tracking System
MIS	Management Information Systems
MS	Microsoft
M&SSI	Materials and Storage Supervisor I
MSS	Material and Storage Supervisor
MTA	Medical Technical Assistant
NCWF	Northern California Womens Facility
NKSP	North Kern State Prison
OBIS	Offender Based Information System
OCR	Office of Community Resources
OIT	Office of Information Technology
OMR	Office of Machine Repair
PED	Policy and Evaluation Division

OP	Operational Procedure
OPF	Official Personnel File
PA	Program Administrator
PASU	Parole Automation Support Unit
PBSP	Pelican Bay State Prison
PC	Penal Code
PC	Partial Compliance
PC	Personal Computer
PCS	Property Control System
P&CSD	Parole and Community Services Division
PDS	Pharmacy Download System
PIA	Prison Industry Authority
PIO	Public Information Officer
PLATO	**find**
PM	Preventive Maintenance
PPAS	Personnel Post Assignment Schedule
PPC	portable personal computer
PPTS	Pharmacy Prescription Tracking System
PVSP	Pleasant Valley State Prison
QA	Quality Assurance
QC	Quality Control
RACF	Resource Access Control Facility
RC	Reception Center
RDT	Random Drug Testing
RJD	Richard J. Donovan Correctional Facility
RN	Registered Nurse
R&R	Receiving and Release
SAC	California State Prison, Sacramento
SAM	State Administrative Manual
SAPMS	Statewide Automated Preventative Maintenance System
SCC	Sierra Conservation Center
SCEP	Supervisor of Correctional Education Program
S&I	Security and Investigations
SISA	Supervisor Information Systems Analyst
SLAMM	Statewide Logistics and Material Management System
SOL	California State Prison, Solano
SQ	California State Prison, San Quentin
SRN	Supervisor Registered Nurse
STD Form 65	Contract/Delegation Purchase Order
SVI	Supervisor of Vocational Instruction
SVSP	Salinas Valley State Prison
TB	Tuberculosis
TB	TB Chronolog Program
TCIP/IP	Transfer Control Protocol/Internet Protocol
TSU	Tactical Support Unit
UA	Urine Analysis
VSPW	Valley State Prison for Women

WOTS	Watch Office Tracking System
WSP	Wasco State Prison